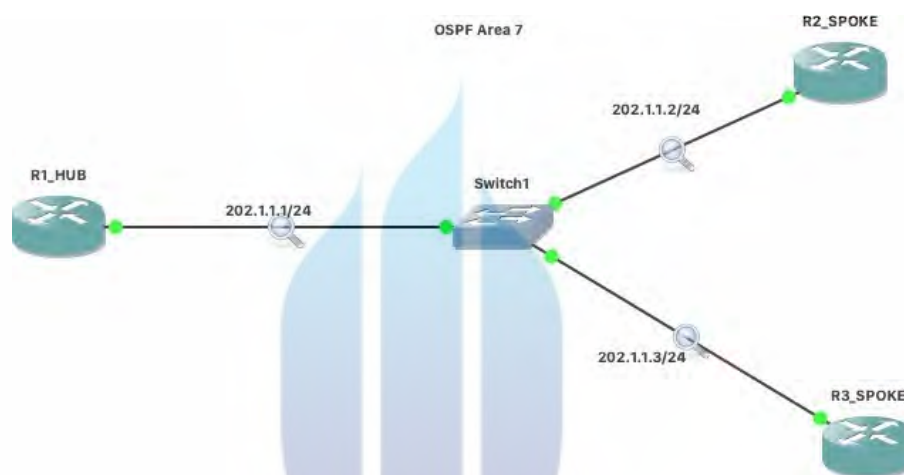


## BAGIAN 4 PERANCANGAN

### 4.1. Skema dan Gambar Kerja

#### 4.1.1. Existing Configuration

Bagian ini menjelaskan mengenai topologi yang sudah ada sebelumnya serta konfigurasi yang digunakan dalam interkoneksi antar *HUB* dan *SPOKE(s)*.

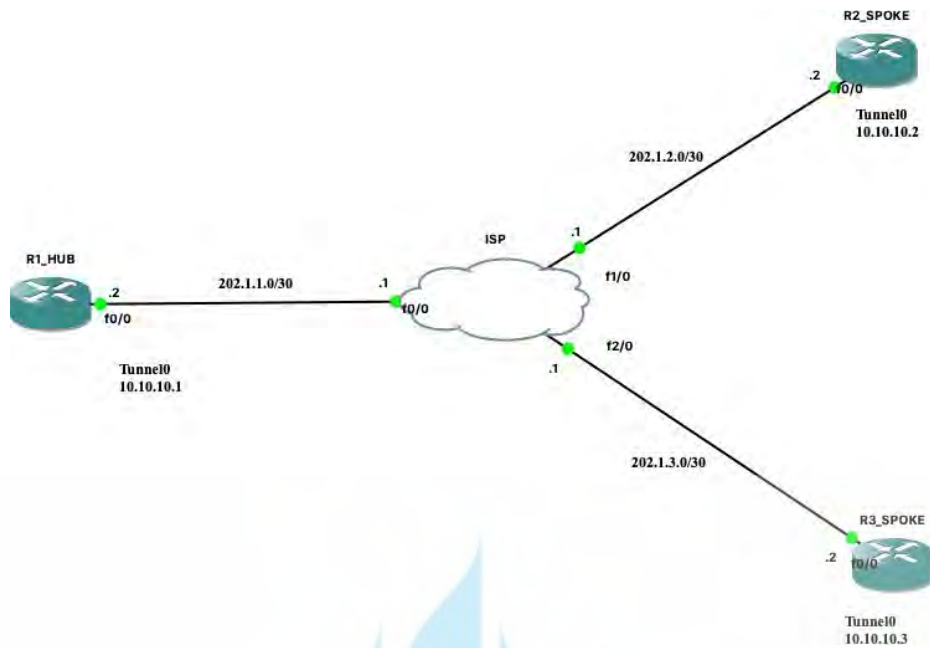


Gambar 7. Topologi jaringan *existing*.

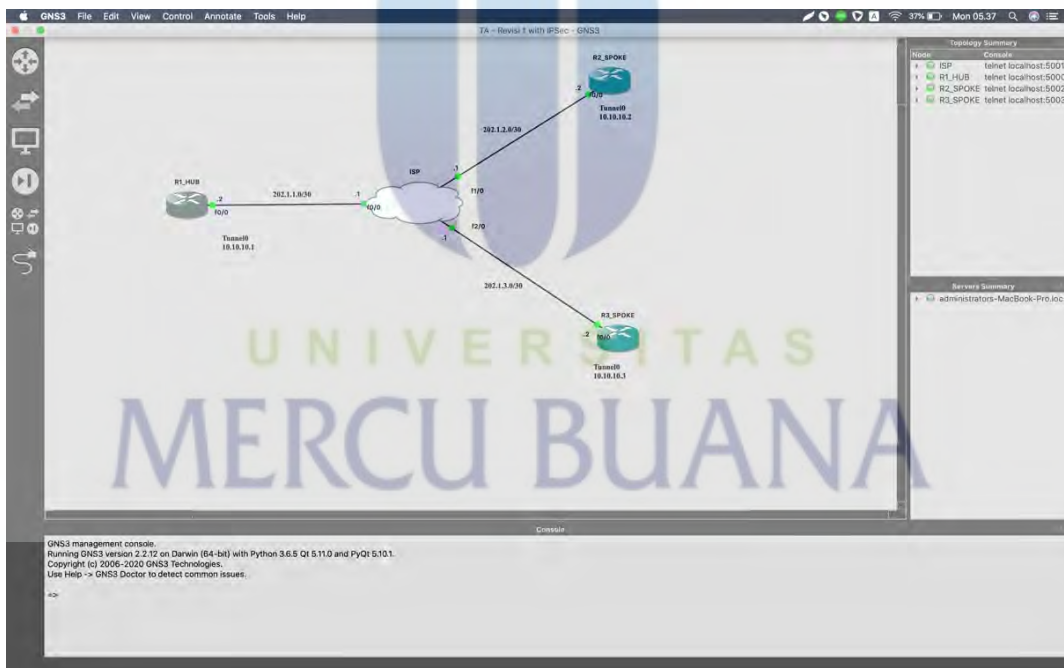
Saat ini, PT.Cahaya Kreatif Digital menggunakan konfigurasi *OSPF* (*Open Shorten Path First*) untuk menghubungkan antar kantor.

#### 4.1.2. Topologi *DMVPN*

Pada bagian ini, topologi serta konfigurasi akan dijelaskan. Berikut ini topologi yang digunakan pada percobaan konfigurasi *DMVPN* menggunakan *IPSec* dan *Routing EIGRP* pada PT. Cahaya Kreatif Digital.



Gambar 8. Topologi jaringan *DMVPN*.



Gambar 9. Topologi jaringan pada GNS3.

Pada topologi jaringan di atas tersedia 3 buah router dan masing-masing diberi nama R1\_HUB, ISP, R2\_SPOKE dan R3\_SPOKE. R1\_HUB adalah *router hub* yang berfungsi sebagai penghubung antara spoke dan dihubungkan dengan ISP. ISP disini dianalogikan sebagai *ISP (Internet Service Provider)*.

R2\_SPOKE dihubungkan dengan ISP agar dapat berkomunikasi dengan R1\_HUB maupun R3\_SPOKE. R3\_SPOKE dihubungkan dengan *router* ISP.

*Tunneling* proses terjadi melalui *router* ISP, antar *router* HUB dan SPOKE. Proses *tunneling* ini membuat transfer data menjadi lebih singkat sebagai contoh apabila R1\_HUB ingin mengirimkan data menuju R2\_SPOKE, seolah-olah antara kedua *router* ini memiliki suatu jalur khusus seperti terowongan yang menghubungkan dua titik. Contoh lainnya, apabila R2\_SPOKE Mengirimkan data menuju R3\_SPOKE ataupun sebaliknya kedua *router* tersebut tidak R1\_HUB untuk berkomunikasi, ke kedua *router* ini memiliki terowongan untuk mentransfer data nya sendiri sehingga proses komunikasi atau transfer data menjadi lebih singkat dan dapat mengurangi beban *router* R1\_HUB.

## 4.2. Konfigurasi Perangkat

Pastikan IOS yang terdapat di dalam keempat *router* tersebut mendukung untuk fitur *DMVPN*. Sebagai contoh apabila kita menggunakan *router* cisco tipe 3725 dan meng-*upgrade* IOS tersebut dengan *module* atau *license boot module security9*.

Setelah perangkat dan bahan disiapkan dan sudah dipasang sesuai topologi langkah selanjutnya yaitu proses konfigurasi tiap *router* dengan memberikan *IP address* dan memasukkan *command-command* terkait. Berikut adalah konfigurasi yang perlu dilakukan untuk menerapkan konfigurasi *DMVPN* menggunakan *IPSec* dan *EIGRP*:

### 4.2.1. Pilih *Router* dan IOS yang dapat mendukung teknologi *DMVPN* dan *EIGRP*

*Router* yang dapat melakukan ini adalah *router* dengan IOS diatas versi duabelas (12) seperti *router* Cisco 881, 1905, 2851, 3725, 7200 dan sebagainya. Apabila, IOS dibawah versi tersebut maka, harus di *upgrade* terlebih dahulu. Berikut ini langkah-langkah meng- *upgrade* module:

- Buka CLI pada *router*.
- Masukkan konfigurasi seperti berikut:

```

R1_HUB#configuration terminal
R1_HUB(config)# license boot module c2900 technology-package securityk9
ACCEPT? [yes/no]: yes
R1_HUB (config)# do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R1_HUB # Reload !untuk me-restart router

```

Tabel 4. Upgrade module

#### 4.2.2. Konfigurasi IP address sesuai topologi

Setelah mendapatkan *router* dan IOS yang sesuai dan sudah diubah *hostname*-nya maka langkah selanjutnya adalah memberikan *IP address* setiap port sesuai dengan topologi yang ada.

```

Router#configure terminal
Router(config)#hostname R1_HUB !Untuk mengubah hostname
R1_HUB(config)#int FastEthernet 0/0 !masuk kedalam interface Fa0/0
R1_HUB(config-if)#ip address 202.1.1.2 255.255.255.252

```

```

R1_HUB(config-if)#speed 100
R1_HUB(config-if)#duplex full
R1_HUB(config-if)#no shutdown !untuk mengaktifkan interface fa0/0
R1_HUB(config)#interface loopback0 !mengaktifkan interface Loopback 0
R1_HUB(config-if)#ip address 192.168.1.1 255.255.255.0
R1_HUB(config-if)#no shutdown
R1_HUB(config-if)#exit
R1_HUB(config)#crypto isakmp policy 1 !DMVPN Phase 1
R1_HUB(config-isakmp)#authentication pre-share
R1_HUB(config-isakmp)#exit
R1_HUB(config)#crypto isakmp key Ckd123! address 0.0.0.0 !harus sama antara hub dan spoke

```

```

R1_HUB(config)#crypto ipsec transform-set TSET esp-des esp-md5-hmac
!DMVPN phase 2

R1_HUB(cfg-crypto-trans)#mode tunnel
R1_HUB(cfg-crypto-trans)#exit
R1_HUB(config)#crypto ipsec profile VPNPROF
R1_HUB(ipsec-profile)#set transform-set TSET
R1_HUB(ipsec-profile)#exit
R1_HUB(config)#interface Tunnel 0 !mengaktifkan interface tunnel 0
R1_HUB(config-if)#ip address 10.10.10.1 255.255.255.0
R1_HUB(config-if)#no ip next-hop-self eigrp 1 !agar router tidak menjadi
next hop
R1_HUB(config-if)#ip nhrp map multicast dynamic
R1_HUB(config-if)#ip nhrp network-id 1 !harus sama antara hub dan spoke
R1_HUB(config-if)#no ip split-horizon eigrp 1
R1_HUB(config-if)#tunnel source FastEthernet0/0
R1_HUB(config-if)#tunnel mode gre multipoint
R1_HUB(config-if)#tunnel key 7777 !harus sama antara hub dan spoke

```

---

**Tabel 5. Konfigurasi R1\_HUB**

Pada konfigurasi R1\_HUB, terdapat inputan *crypto isakmp policy 1* Ini adalah proses input untuk mengaktifkan DMVPN fase pertama. Angka 1 setelah *policy* dapat diubah dengan angka berapa saja tapi perlu diingat angka ini menjadi titik acuan untuk mengkonfigurasi di *router* lainnya. Hal yang perlu diperhatikan selanjutnya adalah *ip nhrp network-id 1*, nhrp harus sama antara semua perangkat router. Nhrp adalah Next-Hop Resolution Protocol. crypto isakmp key Ckd123! address 0.0.0.0 , key ini adalah *password* enkripsi, sehingga perangkat dapat mengenkripsi dan dekripsi pesan dengan *password* yang telah ditentukan.

```

Router#configure terminal
Router(config)#hostname ISP
ISP(config)#interface fastEthernet 0/0
ISP(config-if)#ip address 202.1.1.1 255.255.255.252
ISP(config-if)#speed 100
ISP(config-if)#duplex full
ISP(config-if)#no shutdown
ISP(config)#interface fastEthernet 1/0
ISP(config-if)#ip address 202.1.2.1 255.255.255.252
ISP(config-if)#speed 100
ISP(config-if)#duplex full
ISP(config-if)#no shutdown
ISP(config)#interface fastEthernet 2/0
ISP(config-if)#ip address 202.1.3.1 255.255.255.252
ISP(config-if)#speed 100
ISP(config-if)#duplex full
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP#write

```

**Tabel 6. Konfigurasi ISP**

```

Router#configure terminal
Router(config)#hostname R2_SPOKE
R2_SPOKE(config)#interface fastEthernet 0/0
R2_SPOKE(config-if)#ip address 202.1.2.2 255.255.255.252
R2_SPOKE(config-if)#speed 100
R2_SPOKE(config-if)#duplex full
R2_SPOKE(config-if)#no shutdown
R2_SPOKE(config)#crypto isakmp policy 1
R2_SPOKE(config-isakmp)#authentication pre-share
R2_SPOKE(config-isakmp)#exit
R2_SPOKE(config)#crypto isakmp key Ckd123! address 0.0.0.0

```



```

R2_SPOKE(config)#crypto ipsec transform-set TSET esp-des esp-md5-
hmac
R2_SPOKE(cfg-crypto-trans)#mode tunnel
R2_SPOKE(cfg-crypto-trans)#exit
R2_SPOKE(config)#crypto ipsec profile VPNPROF
R2_SPOKE(ipsec-profile)#set transform-set TSET
R2_SPOKE(ipsec-profile)#exit
R2_SPOKE(config)#interface Tunnel 0
R2_SPOKE(config-if)#ip address 10.10.10.2 255.255.255.0
R2_SPOKE(config-if)#ip nhrp map 10.10.10.1 201.1.1.1
R2_SPOKE(config-if)#ip nhrp map multicast 201.1.1.1
R2_SPOKE(config-if)#ip nhrp network-id 1
R2_SPOKE(config-if)#ip nhrp nhs 10.10.10.1
R2_SPOKE(config-if)#tunnel source FastEthernet0/0

```

```

R2_SPOKE(config-if)#tunnel mode gre multipoint
R2_SPOKE(config-if)#tunnel key 7777
R2_SPOKE(config-if)#tunnel protection ipsec profile VPNPROF
R2_SPOKE(config)#router eigrp 1
R2_SPOKE(config-router)#network 192.168.2.0
R2_SPOKE(config-router)#network 10.0.0.0
R2_SPOKE(config-router)#exit
R2_SPOKE(config)#ip route 0.0.0.0 0.0.0.0 202.1.1.5
R2_SPOKE(config)#exit
R2_SPOKE#write

```

**Tabel 7. Konfigurasi R2\_SPOKE**

```
Router#configure terminal
Router(config)#hostname R3_SPOKE
R3_SPOKE(config)#interface fastEthernet 0/0
R3_SPOKE(config-if)#ip address 202.1.3.2 255.255.255.252
R3_SPOKE(config-if)#speed 100
R3_SPOKE(config-if)#duplex full
R3_SPOKE(config-if)#no shutdown
R3_SPOKE(config)#crypto isakmp policy 1
R3_SPOKE(config-isakmp)#authentication pre-share
R3_SPOKE(config-isakmp)#exit
R3_SPOKE(config)#crypto isakmp key Ckd123! address 0.0.0.0
R3_SPOKE(config)#crypto ipsec transform-set TSET esp-des esp-md5-
hmac
R3_SPOKE(cfg-crypto-trans)#mode tunnel
R3_SPOKE(cfg-crypto-trans)#exit
R3_SPOKE(config)#crypto ipsec profile VPNPROF
R3_SPOKE(config-profile)#set transform-set TSET
R3_SPOKE(config-profile)#exit
```

UNIVERSITAS  
MERCU BUANA



```

R3_SPOKE(config)#interface Tunnel 0
R3_SPOKE(config-if)#ip address 10.10.10.3 255.255.255.0
R3_SPOKE(config-if)#ip nhrp map 10.10.10.1 202.1.1.1
R3_SPOKE(config-if)#ip nhrp map multicast 202.1.1.1
R3_SPOKE(config-if)#ip nhrp network-id 1
R3_SPOKE(config-if)#ip nhrp nhs 10.10.10.1
R3_SPOKE(config-if)#tunnel source FastEthernet0/0
R3_SPOKE(config-if)#tunnel mode gre multipoint
R3_SPOKE(config-if)#tunnel key 7777
R3_SPOKE(config-if)#tunnel protection ipsec profile VPNPROF
R3_SPOKE(config)#router eigrp 1
R3_SPOKE(config-router)#network 10.0.0.0
R3_SPOKE(config-router)#network 192.168.3.0
R3_SPOKE(config-router)#exit
R3_SPOKE(config)#ip route 0.0.0.0 0.0.0.0 202.1.1.9
R3_SPOKE(config)#exit
R3_SPOKE#write

```

**Tabel 8. Konfigurasi R3\_SPOKE**

#### 4.3. Verifikasi Hasil

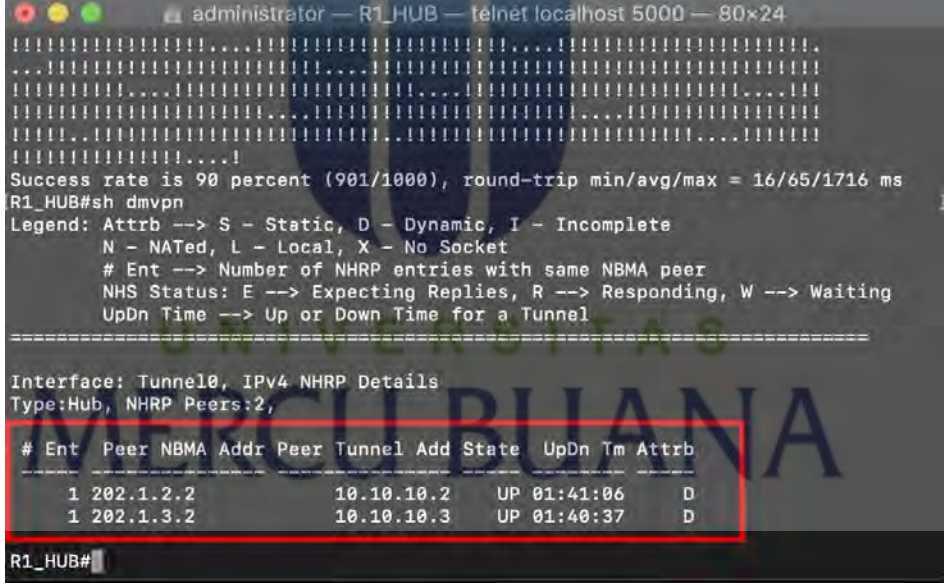
Verifikasi hasil merupakan proses pengecekan konfigurasi yang telah kita masukkan, verifikasi tersebut berupa *show command* terkait dan dengan melakukan *test ping*, *traceroute* dan *debug*. Tujuan verifikasi hasil ini adalah untuk mengetahui apakah konfigurasi yang kita lakukan sudah berhasil seperti rencana semula atau belum. Berikut ini adalah hasil verifikasi DMVPN dari R1\_HUB, ISP, R2\_SPOKE, R3\_SPOKE.

4.3.1. Verifikasi Hasil R1\_HUB

```
R1_HUB#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       # Ent --> Number of NHRP entries with same NBMA neer

Tunnel0, Type:Hub, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
      1      202.1.1.6     10.10.10.2    UP   never D
      1      202.1.1.10    10.10.10.3    UP   never D
```

**Tabel 9. Hasil test R1\_HUB**



```
administrator — R1_HUB — telnet localhost 5000 — 80x24
.....
.....
.....
.....
.....
.....
.....
.....
.....!
.....!
.....!
.....!
.....!
.....!
Success rate is 90 percent (901/1000), round-trip min/avg/max = 16/65/1716 ms
R1_HUB#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       # Ent --> Number of NHRP entries with same NBMA peer
       NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
       UpDn Time --> Up or Down Time for a Tunnel

-----

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
  1 202.1.2.2      10.10.10.2    UP 01:41:06 D
  1 202.1.3.2      10.10.10.3    UP 01:40:37 D

R1_HUB#
```

**Gambar 10. Show dmvpn R1\_HUB**









### 4.3.3. Verifikasi Hasil *R3\_SPOKE*

```

R3_SPOKE#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
          N - NATed, L - Local, X - No Socket
          # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Spoke, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
          1          202.1.1.1          10.10.10.1          UP 00:03:41 S

```

**Tabel 11. Hasil test *R3\_SPOKE***

```

administrator — R3_SPOKE — telnet localhost 5003 — 80x24
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 88 percent (889/1000), round-trip min/avg/max = 16/69/1652 ms
R3_SPOKE#sh dmv
R3_SPOKE#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
          N - NATed, L - Local, X - No Socket
          # Ent --> Number of NHRP entries with same NBMA peer
          NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
          UpDn Time --> Up or Down Time for a Tunnel
=====
Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
-----
          1 202.1.1.2          10.10.10.1          UP 01:46:34          S
          1 202.1.2.2          10.10.10.2          UP 01:30:39          D
R3_SPOKE#

```

**Gambar 16. Show dmvpn pada *R3\_SPOKE***





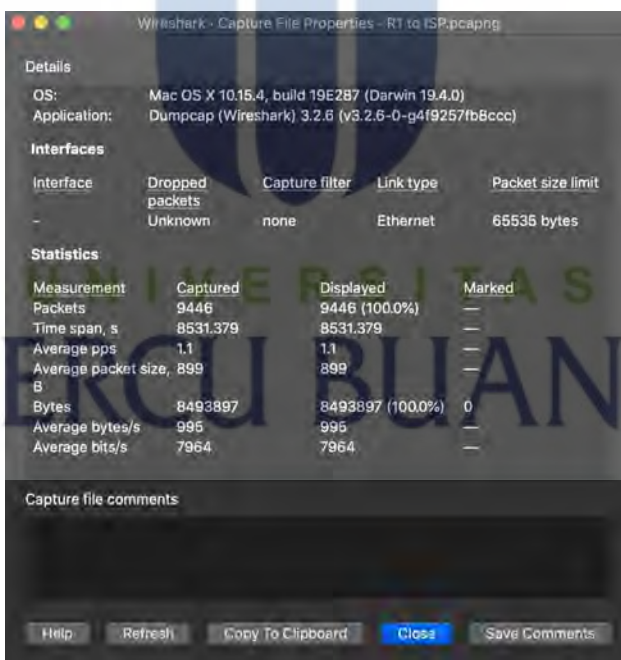
secara dinamis kita bisa mengetahuinya dari *Attrb*, hub akan menyimpan semua *IP Private* dan *IP Public* dari setiap spoke, sedangkan pada spoke kita hanya mengetahui *IP Private* dan *IP Public* dari hub.

#### 4.4. Pengujian

Pada bagian ini, menjelaskan mengenai konfigurasi DMVPN. Pengujian ini menghasilkan *ping*, *jitter*, *package loss*, dan *next-hop* yang dilalui oleh paket data.

##### 4.4.1. Hasil *Throughput*

Hasil *throughput* menunjukkan kecepatan data di transfer sesungguhnya. Throughput adalah jumlah total kedatangan packet yang berhasil diamati pada tujuan selama interval tertentu.



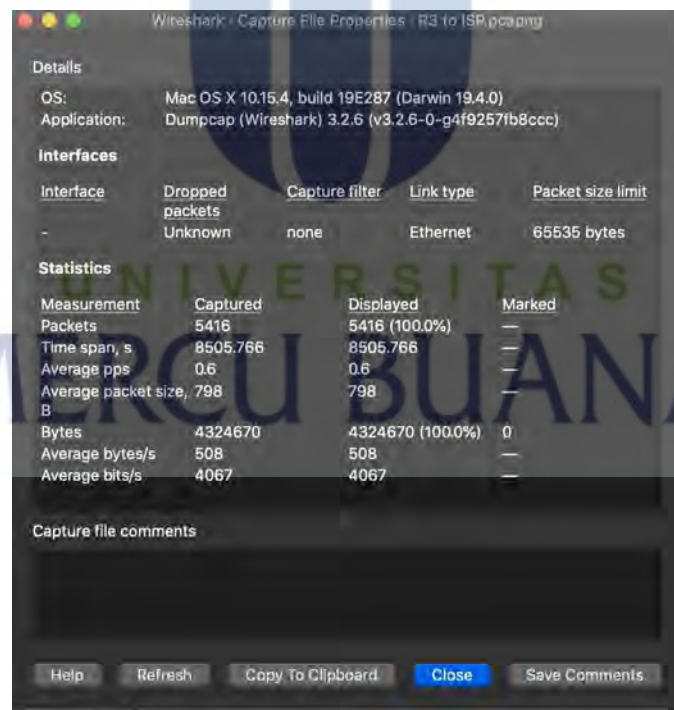
The screenshot shows the 'Statistics' section of the Wireshark dialog box. The data is as follows:

Measurement	Captured	Displayed	Marked
Packets	9446	9446 (100.0%)	—
Time span, s	8531.379	8531.379	—
Average pps	1.1	1.1	—
Average packet size, B	899	899	—
Bytes	8493897	8493897 (100.0%)	0
Average bytes/s	995	995	—
Average bits/s	7964	7964	—

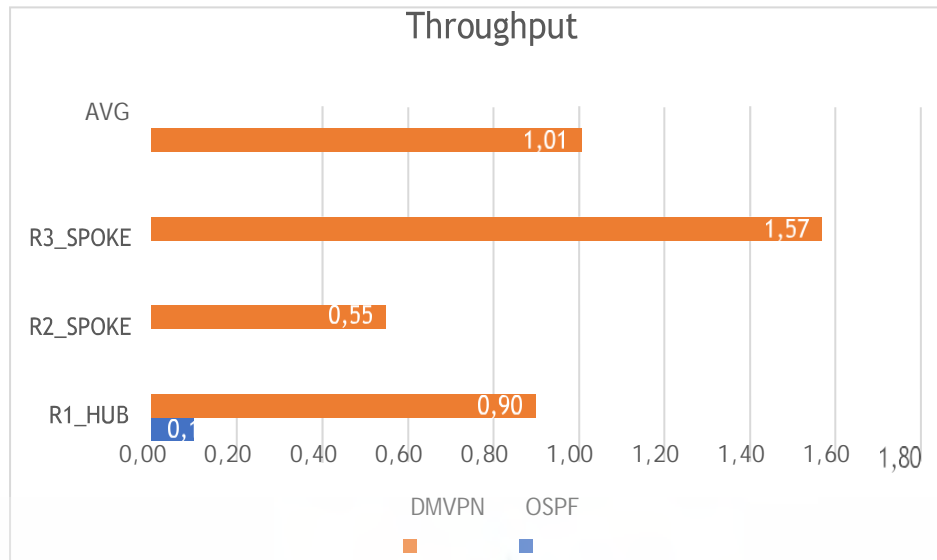
**Gambar 19. Throughput dari R1 to ISP**



Gambar 20. Throughput dari R2 to ISP



Gambar 21. Throughput dari R3 to ISP



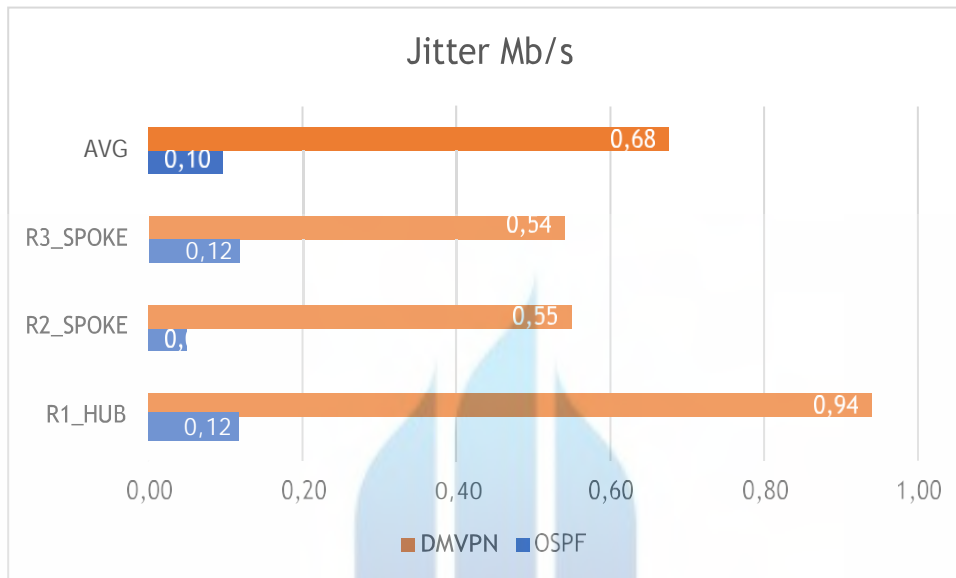
**Gambar 22. Perbandingan hasil throughput.**

Dari percobaan diatas, dapat disimpulkan bahwa penggunaan DMVPN lebih effisien dalam proses transfer data. *Throughput* DMVPN secara rata-rata memiliki kecepatan 1,01Mbps sedangkan OSPF memiliki kecepatan rata-rata 0,26Mbps. DMVPN lebih cepat dan effisien sekitar 74.17%.

UNIVERSITAS  
MERCU BUANA

#### 4.4.2. Hasil Jitter

*Jitter* dapat didefinisikan sebagai variasi-variasi *delay* antar *block-block* yang berutan. Besarnya nilai jitter sangat berpengaruh oleh variasi-variasi beban trafik dan besarnya tumpukan antar *packet*.



**Gambar 23. Perbandingan hasil jitter**

Pada data diatas, *jitter* pada DMVPN lebih besar dibanding OSPF dengan perbedaan rata-rata 0,68Mbps.

MERCU BUANA